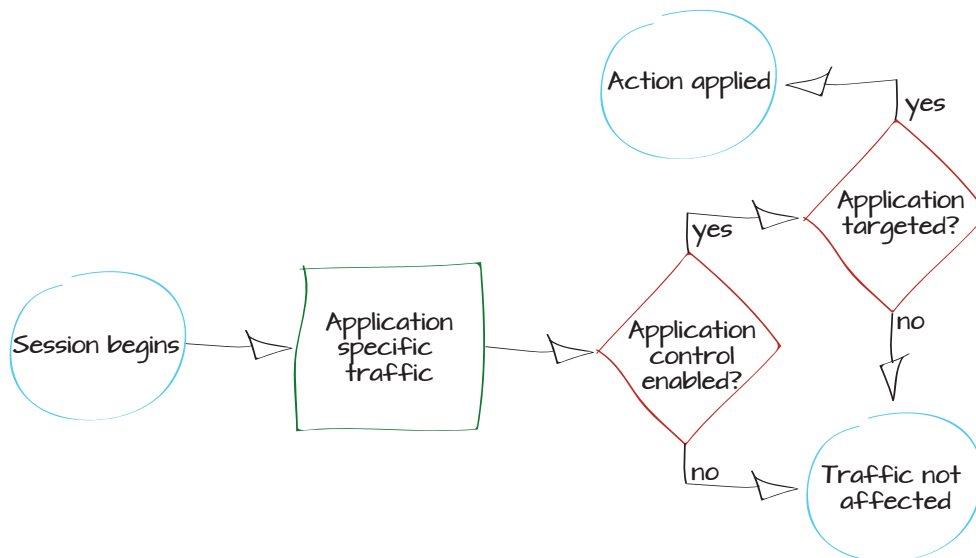


# Controlling which applications can access network resources and the Internet

In this example, you will learn how to use Application Control to monitor traffic and determine if there are any applications currently in use that should not have network access. If you discover any applications that you wish to block, application control will then be used to ensure that these applications cannot access the network.

1. Enabling Application Control and multiple security profiles
2. Using the default application profile to monitor network traffic
3. Adding the default profile to a security policy
4. Reviewing the FortiView dashboards
5. Creating an application profile to block applications
6. Adding the blocking sensor to a security policy
7. Results



## 1. Enabling Application Control and multiple security profiles

Go to **System > Config > Features** and ensure that **Application Control** is turned **ON**.



Select **Show More** and enable **Multiple Security Profiles**.

**Apply** the changes.

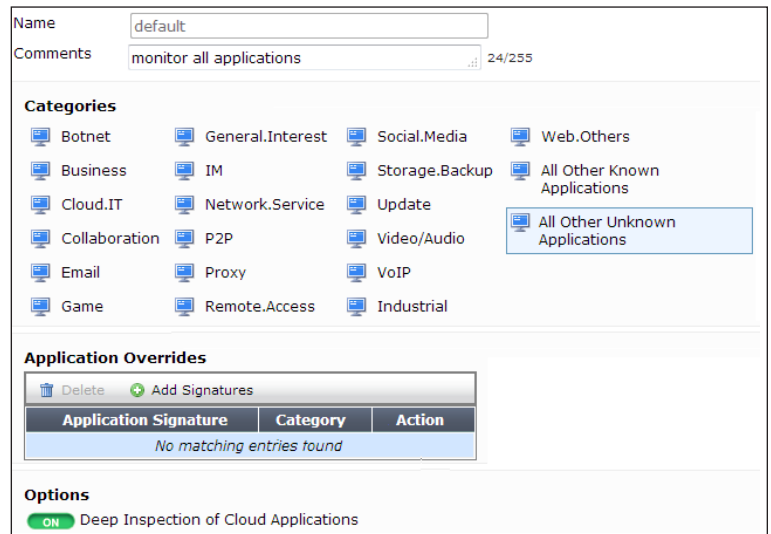


## 2. Using the default application profile to monitor network traffic

Go to **Security Profiles > Application Control** and view the **default** profile.

A list of application **Categories** is shown. By default, most categories are already set to **Monitor**. In order to monitor all applications, select **All Other Known Applications** and set it to Monitor. Do the same for **All Other Unknown Applications**.

The default profile also has **Deep Inspection of Cloud Applications** turned **ON**. This allows web-based applications, such as video streaming, to be monitored by your FortiGate.



3. Adding the default profile to a security policy

Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows outgoing traffic from your network.

Under **Security Profiles**, turn on **Application Control** and use the **default** profile.

Enabling Application Control will automatically enable **SSL Inspection**. In order to inspect traffic from Cloud Applications, the **deep-inspection** profile must be used.



Using the **deep-inspection** profile may cause certificate errors. For information about avoiding this, see “[Preventing security certificate warnings when using SSL full inspection](#)” on page 63.

Incoming Interface

internal

Source Address

all

Source User(s)

Click to add...

Source Device Type

Click to add...

Outgoing Interface

wan1

Destination Address

all

Schedule

always

Service

ALL

Action

ACCEPT

Firewall / Network Options

ON

 NAT

Use Destination Interface Address

Use Dynamic IP Pool

Fixed Port

Click to add...

Security Profiles

OFF

 AntiVirus

default

OFF

 Web Filter

default

ON

 Application Control

default

OFF

 IPS

default

ON

 SSL Inspection

certificate-inspection

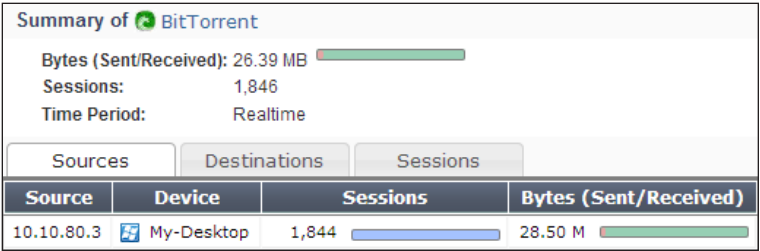
4. Reviewing the FortiView dashboards

Go to **System > FortiView > Applications** and select the **now** view.

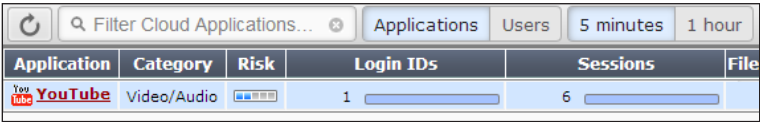
This dashboard shows the traffic that is currently flowing through your FortiGate, arranged by application (excluding Cloud Applications).

Filter Applications...					now	5 minutes	1 hour
Application	Category	Risk	Sessions	Bytes (Sent/Received)			
BitTorrent	P2P		78	410.37 K			
DNS	Network.Service		66	16.94 K			
SSL	Network.Service		21	16.04 M			
Skype	P2P		13	273.90 K			
Unknown			6	442			
Twitter	Social.Media		3	29.61 K			
LastPass	Storage.Backup		1	23.05 K			

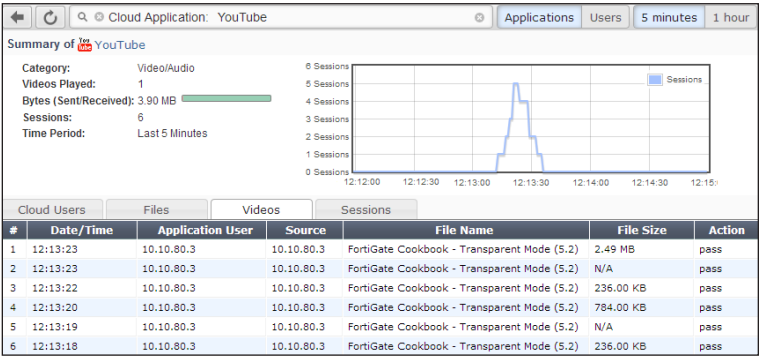
If you wish to know more about an application's traffic, double-click on its entry to view drilldown information, including traffic sources, traffic destinations, and information about individual sessions.



Similar information can be viewed for Cloud Applications by going to **System > FortiView > Cloud Applications** and selecting **Applications** that have been used in the last **5 Minutes**.



Cloud Applications also have drilldown options, including the ability to see which videos have been viewed if streaming video traffic was detected.



5. Creating an application profile to block applications

In the above example, traffic from BitTorrent, a Peer-to-Peer (P2P) downloading application, was detected. Now, you will create an application control profile that will block P2P traffic.

The new profile will also block all applications associated with Youtube, without blocking other applications in the **Video/Audio** category.

Go to **Security Profiles > Application Control** and create a new profile.

Select the **P2P** category and set it to **Block**.

Categories

☒

 Botnet

☒

 Business

☒

 Cloud.IT

☒

 Collaboration

☒

 Email

☒

 Game

☒

 General.Interest

☒

 IM

☒

 Network.Service

☒

 P2P

☒

 Proxy

☒

 Remote.Access

Under **Application Overrides**, select **Add Signatures**.

























**Search** for *Youtube* and select all the signatures that are shown.

Select **Use Selected Signatures**.

Youtube				
Application Name	Category	Technology	Popularity	Risk
YouTube	Video/Audio	Browser-Based	☆☆☆☆☆	Low
YouTube.App	Video/Audio	Client-Server	☆☆☆☆☆	Low
Youtube.Downloader.YTD	Video/Audio	Client-Server	☆☆☆☆☆	Low
YouTube_Comment.Posting	Video/Audio	Browser-Based	☆☆☆☆☆	Low
YouTube_HD.Streaming	Video/Audio	Browser-Based	☆☆☆☆☆	Low
YouTube_Search.Safety.Mode.Off	Video/Audio	Browser-Based	☆☆☆☆☆	Low
YouTube_Search.Video	Video/Audio	Browser-Based	☆☆☆☆☆	Low
YouTube_Video.Access	Video/Audio	Browser-Based	☆☆☆☆☆	Low
YouTube_Video.Embedded	Video/Audio	Browser-Based	☆☆☆☆☆	Low
YouTube_Video.Play	Video/Audio	Browser-Based	☆☆☆☆☆	Low
YouTube_Video.Upload	Video/Audio	Browser-Based	☆☆☆☆☆	Low
Youtubeproxyfree	Proxy	Browser-Based	☆☆☆☆☆	High

The signatures have been added to the Application Overrides list and have automatically been set to Block.

Enable **Deep Inspection of Cloud Applications**.

Delete + Add Signatures		
Application Signature	Category	Action
 YouTube	Video/Audio	 Block
 YouTube.App	Video/Audio	 Block
 Youtube.Downloader.YTD	Video/Audio	 Block
 YouTube_Comment.Posting	Video/Audio	 Block
 YouTube_HD.Streaming	Video/Audio	 Block
 YouTube_Search.Safety.Mode.Off	Video/Audio	 Block
 YouTube_Search.Video	Video/Audio	 Block
 YouTube_Video.Access	Video/Audio	 Block
 YouTube_Video.Embedded	Video/Audio	 Block
 YouTube_Video.Play	Video/Audio	 Block
 YouTube_Video.Upload	Video/Audio	 Block
 Youtubeproxyfree	Proxy	 Block
<b>Options</b>		
<input checked="" type="checkbox"/> Deep Inspection of Cloud Applications		

## 6. Adding the blocking sensor to a security policy

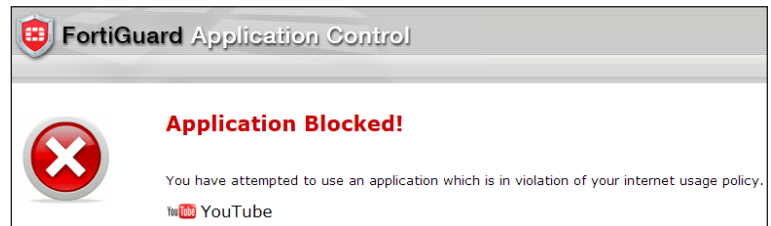
Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows outgoing traffic from your network.

Set **Application Control** to use the new profile.

Security Profiles	
<input checked="" type="checkbox"/> AntiVirus	default
<input type="checkbox"/> Web Filter	default
<input checked="" type="checkbox"/> Application Control	block-applications

## 7. Results

Attempt to browse to [www.youtube.com](http://www.youtube.com). A warning message will appear, stating that the application was blocked.



Traffic from BitTorrent applications will also be blocked.

To see information about this blocked traffic, go to **System > FortiView > All Sessions**, select the **5 minutes** view, and filter the traffic by application.

		Application: BitTorrent		now	5 minutes	1 hour
#	Date/Time	Source	Device	Application Name	Security Action	Security Event
1	14:09:33	10.10.80.3	My-Desktop	BitTorrent	Blocked	1
2	14:09:26	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
3	14:09:19	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
4	14:09:16	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
5	14:09:12	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
6	14:09:05	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
7	14:08:58	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
8	14:08:51	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
9	14:08:44	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
10	14:08:37	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
11	14:08:30	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1